IDENTIFICATION OF PHYSICAL SECURITY SYSTEMS

Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Instructions: This checklist identifies the physical security elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Physical Security System Element	Element Present		COMMENTS
	Yes	No	
Perimeter Barriers			
Building Barriers			
Intrusion Detection			
Access Controls			
Security Force			

IDENTIFICATION OF PROCESS SAFETY SYSTEMS

Date: [MONTH XX, 2002] Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]
Instructions: This checklist identifies the process safety elements that may be used to protect the entire facility and/or a critical asset. Identify which elements are present for the facility or the critical asset listed above. Once physical security elements are identified, they can be reviewed by using the applicable checklists. At the completion of the reviews, the effectiveness of the elements is to be documented in the body of the survey report.

Process Safety System Element	Element Present		COMMENTS
	Yes	No	
Hardening Processes			
Emergency Response			
Chemical Detection			
Fire Detection			
Fire Suppression			

SECURITY PROGRAM MANAGEMENT

Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(a) Security Organization	
1. Is there a senior level security working group with representatives from each major office or department to establish security policies (including physical security, operations security, and infrastructure interdependencies security) and integrate them across all elements of the organization? • If there is a senior level security working group, describe the membership, the lines of communication, and any scheduled periodic meetings to resolve security issues. • If there is not such a group, how are security policies established?	
2. Is there a security office that is responsible for implementing security policies and procedures (including physical security, operations security, and infrastructure interdependencies security)? • If there is a security office, where does it report in the organization, how many people are in the office, and are resources adequate? Also describe any training received. • If there is not such an office, how are security policies implemented?	
(b) Security Plans and Policies	
3. Is there a mission statement describing the physical security, operations security, and infrastructure security programs?	
4. Is there a formal security plan and statement of security policies? If there is, describe it including how it is communicated to employees.	
5. Is there a formal threat definition and assessment statement? If there is, describe it including how it is communicated to employees.	

SECURITY PROGRAM MANAGEMENT (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(c) Security Resources	
1. Are the resources (budget and staffing) applied to security (including physical security, operations security, and infrastructure interdependencies security) considered adequate?	
2. Do security personnel feel that they have adequate training to accomplish their functions?	
(d) Senior Management Security	
1. Is there an executive protection program for senior executives/managers? If there is such a program, describe it.	
2. Is public information on senior executives/managers controlled? If it is, describe how it is controlled.	
(e) Security Audits	
1. Is there a regular security assessment or audit? If there is, describe how it is done, by whom, and how frequently.	
2. Has the most recent audit indicated any weaknesses? Summarize the results of the audit, particularly any weaknesses identified.	
3. Have any corrective measures been implemented recently? Describe them.	
(f) Handling of Sensitive Information	
1. How is sensitive information identified and marked?	
2. Who has access to sensitive security information?	
3. How is sensitive information protected, stored, accessed, transmitted, and destroyed?	
4. How do senior executives/managers protect sensitive security information?	

SECURITY PROGRAM MANAGEMENT (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
	COMMENTS
(g) Internal Communications	
1. How does management provide security information to employees at the site?	
2. Describe the process for obtaining feedback from employees on security related issues.	

THREAT DETECTION AND EVALUATION CAPABILITIES

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
(a) Threat Analysis Working Group	
1. Is the organization a member of a local threat analysis working group? Describe the group	
2. If the organization is a member of such a group, list the organizations that participate in the working group (e.g., local, county, state, and federal agencies, the military).	
3. Are there other industry partners participating in the working group? Describe them.	
4. Are active efforts being made to recruit other meaningful participants into the working group? Describe the efforts.	
5. Do the participants in the working group have management support, requirements, and funding to participate? Describe the situation.	
6. Are the members of the working group willing participants and do they work against bureaucratic obstacles that may prevent the success of the group? Describe the situation.	
7. Do the members of the working group have the authority to share information with other members of the group? Describe the situation.	
8. Have the members of the working group been given appropriate U.S. government clearances to share in threat information? Describe the situation.	
9. Do the members of the working group have access to the National Infrastructure Protection Center (NIPC), Analytical Services, Inc., (ANSER), FBI-sponsored InfraGuard, Carnegie Mellon University's CERT®, and other information system security warning notices? List the threat information systems they use.	

THREAT DETECTION AND EVALUATION CAPABILITIES (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
10. Indicate the frequency and regularity of the working group meetings.	
11. Do the members of the working group have processes in place to obtain real-time information from the field (e.g., on-duty offices, civilian neighborhood watch programs, local businesses, other working groups in the area)? Describe these processes.	
12. Do members of the working group have the ability to initiate information-gathering requests back into the field environment? Describe the capability.	
13. Are the threat statements developed by the working group specific to the organization or the industry, versus general nationwide warnings? Describe the process for gathering these statements.	
14. Do some members of the working group conduct scheduled meetings with the public to discuss concerns and observations? Describe these interactions.	
15. Do the members of the working group know what the critical assets of the organization are? Describe the extent of their knowledge.	
16. Do the members of the working group understand industry interdependencies and work with other industry members to address these potential concerns? Describe the extent of these interactions.	
17. What are the roles and responsibilities of the working group members during response and recovery activities?	

THREAT DETECTION AND EVALUATION CAPABILITIES (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to the entire facility	
	COMMENTS
(b) Organization's Response to Threat Updates	
1. Does senior management support and/or participate in the threat analysis working group? Describe the extent of the support/ participation.	
2. Does the organization receive as-needed threat briefings from local, state, and federal agencies? Describe the nature and extent of the briefings.	
3. Does the organization have the ability to distribute organization-specific threat warnings in real time? Describe the process.	
4. Does the organization have the ability to augment security programs based on threat updates? Describe the process.	
5. Does the organization conduct historical trending analysis for security events (both planned and actual) and implement security activates to mitigate them? Describe the analysis.	
6. Does the organization create possible threat scenarios based on input from the threat analysis working group and conduct related security exercises? Describe the exercises.	

PERIMETER BARRIERS – FENCES, GATES

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Fences	
1. Characterize fence construction and rate the level of security it provides as low, moderate to high, or other (specify). • Low: no fence or only a 6-foot chain-link fence. • Moderate to high: 8-foot chain-link fence with outriggers, 10 to 12-foot chain-link fence, or over 12-foot chain-link fence with outriggers.	
2. Characterize fence signage as no signs, posted "No Trespassing," or other (specify).	
3. Characterize the fence alarm system as no alarms, fence sensors (taut wire, vibration, strain, electric field, or multiple sensors), or other (specify).	
4. Fence area: • Is the fence within 2 inches of firm hard ground? • Is the fence line clear of vegetation, trash, equipment, and other objects that could impede observation? • Is the area free of objects that would aid in traversing the fence? • Is physical protection installed for all points where utilities (e.g., electric power lines, natural gas pipelines, telecommunication lines, water supply, storm sewers, drainage swells) intersect the fence perimeter?	
5. How is the fence protected from vehicles (aircraft cable, concrete barriers or median, guard rails, steel posts, a ditch, crash I-beams, train barrier, or other [specify])?	
6. Fence illumination: • Is there security lighting for the fences? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	

PERIMETER BARRIERS – FENCES, GATES (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(b) Gates	
1. Characterize the gates as no gate closure, vehicle bar, chain-link fence, or other (specify).	
2. Characterize the gate locks as no lock, lock not used, gate unlocked, gate attended by personnel when unlocked, ID actuated lock, padlock, or other (specify).	
3. How is access to gate keys controlled?	
4. Gate lighting: • Describe the security lighting for the gates. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	
(c) Vehicle Barriers	
1. Characterize vehicle barriers as none, a vehicle bar, blocked by vehicle when gate open, hydraulic wedge, or other (specify).	

BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Walls	
2. Characterize wall construction and rate the level of security wall provide as low, moderate, or high. • Low: chain-link mesh, 16-gauge metal, wood studs and dry wall, wood studs and plywood, or other (specify). • Moderate: clay block, 8-inch hollow block, 8-inch filled block, or other (specify). • High: 8-inch filled rebar block, 12-inch filled rebar block, 2-inch precast concrete tees, 4-inch reinforced concrete, 8-inch reinforced concrete, 12-inch reinforced concrete, 24-inch reinforced concrete, or other (specify).	
3. Do the walls extend from the floor to the structural ceiling?	
(b) Roof/Ceiling	
1. Characterize the roof material and rate the level of security it provides as low, moderate, or high. • Low: 20-gauge metal with insulation, 1/2-inch wood, or other (specify). • Moderate: 20-gauge metal built-up roof, concrete built-up roof with T-beams, or other (specify). • High: 5-1/2-inch concrete roof, 8-inch concrete roof, 3-foot earth cover, 3-foot soil/cement/earth cover, or other (specify).	
2. Does the interior drop ceiling extend beyond the structural walls?	
(c) Windows	

BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
1. Characterize the window materials and rate the level of security they provide as low or moderate. • Low: standard windows or other (specify). • Moderate: 9-gauge expanded mesh, 1/2-inch diameter x 1-1/2-inch quarry screen, 1/2-inch diameter bars with 6-inch spacing, 3/16-inch x 2-1/2-inch grating, or other (specify).	
2. Characterize the window alarms (for windows that would be accessible by foot or ladder) as none, vibration sensor, glass breakage sensor, conducting tape, grid mesh, multiple sensors, or other (specify).	
(d) Doors	
1. Characterize door materials and rate the level of security they provide as low, moderate, or high. • Low: wood, 9-gauge wire mesh, hollow-core metal, no lock/hinge, or other (specify). • Moderate: hollow-core metal, tempered-glass panel, security-glass panel, half-height turnstile, or other (specify). • High security: 1/2-inch steel plate, turnstile – aluminum, Class V or VI vault, or other (specify).	
2. Characterize the door locks and rate the level of security they provide as low, moderate, or high. • Low: none, lock not used, or other (specify). • Moderate: door unlocked, attended by personnel when unlocked, ID actuated lock, padlock, keyed cylinder lock, combination lock, mechanically coded lock, or other (specify). • High: electronically coded lock, two-person rule lock system, lock inaccessible from the door exterior, or other (specify).	

BUILDING BARRIERS – WALLS, ROOF/CEILING, WINDOWS, DOORS (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
3. How is access to the keys for the door locks controlled?	
4. Door Alarms: • Is door position monitored? • Indicate the type of door penetration sensor (vibration, glass breakage, conducting tape, grid mesh, or other [specify]).	

INTRUSION DETECTION

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Intrusion Sensors (If Applicable)	
1. Characterize the exterior intrusion sensors as seismic buried cable, electric field, infrared, microwave, video motion, or other (specify).	
2. Characterize the interior intrusion sensors as sonic, capacitance, video motion, infrared, ultrasonic, microwave, or other (specify).	
(b) Intrusion Alarm Deployment (If Applicable)	

1. Characterize intrusions alarm deployment in terms such as: • continuously monitored, • positioned to prevent gaps in coverage, • detection zone kept clear of obstructions (e.g., dips, equipment, snow, ice, grass, debris), • tamper and system problem indicators provided, • compensatory measures employed when alarms are not operating, • backup power provided, and • other (specify).	
(c) Intrusion Alarm Assessment	
1. Characterize the assessment of intrusion alarms as not assessed, closed circuit TV, automatic deployment of protective force, or other (specify).	

CLOSED CIRCUIT TELEVISION

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(a) CCTV	
1. Describe the current CCTV system in use at the site.	
2. Characterize cameras in use and what asset(s) the cameras cover (PTZ, Autodome type, Fixed, Day/Night)	
3. Who monitors the CCTV cameras (Operations and/or Security) and what are the protocols for camera operation?	

4. Describe the policy for review of information recorded on CCTV system.	
5. Describe the preventive maintenance program for the CCTV system.	

ACCESS CONTROL

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(a) Personnel Access	
1. Characterize access point control as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the identification check process as none in place, casual recognition, credential check (e.g., drivers license, passport, state ID), picture badge, PIN, exchange badge, retinal scan, hand geometry, speech pattern, signature dynamics, fingerprint, or other (specify).	
3. Characterize the organization's badging policy in terms such as no badging policy, visitor badges required, badge issuance and control procedures in place (describe), and badges show permission to access specific areas (describe).	
(b) Vehicle Access	
1. Characterize vehicle access point controls as unmanned, unarmed guard, armed guard, or other (specify).	
2. Characterize the vehicle access identification process as none in place, vehicle stickers, vehicle stickers with personnel identification, automated system (describe), or other (specify).	
3. Describe the vetting process for incoming/outgoing bulk shipments of items by vehicle. Are deliveries scheduled or are is a list of drivers provided prior to delivery.	

ACCESS CONTROL (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
Note: Different access points to the facility and/or to critical assets may have different access controls. The comments should clearly distinguish whether the evaluation applies to all access points or to specific access points.	
	COMMENTS
(c) Contraband Detection	
1. Characterize item and vehicle search procedures as none, cursory, or detailed	
2. Is there a policy for incoming/outgoing drivers that report the possession of weapons? If so describe the policy/procedure.	
(d) Access Point Illumination	
1. Access Point Illumination: • Is there security lighting for the access points? Describe the security lighting system. • Do alarms or infrared detectors trigger the lighting? Describe the triggering process.	

SECURITY FORCE

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Protective Force	
1. Specify the size of the protective force in terms or total number and the number on duty during working hours, non-working hours, and weekends/holidays.	
2. Specify the equipment available to the protective force such as uniforms; vehicles (specify number); weapons (describe); communications devices (describe); and other equipment (describe).	
3. Describe the training of the protective force. Specifically, describe the initial training, any continuing training (e.g., on-the-job), and drills and exercises.	
4. Describe the organization of the protective force. Specifically, describe the command structure, their mission as defined, any established policies and procedures, and established emergency response plans.	
5. Are there provisions for a back-up force (e.g., recalling off-duty personnel)? Describe the provisions in place.	
6. Protective Force Command Center: • Is there a protective force command and control center? Describe it. • Is there a backup center? Describe it.	
7. Are protective force operations disguised to prevent intelligence about the facility from being inadvertently released? Describe how this is done.	
8. Describe protective force procedures for responding to alarms.	
9. Does the protective force provide security escort for visitors? Describe the nature of the escort.	

SECURITY FORCE (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(b) Local Law Enforcement Agencies	
1. Describe the interaction of the protective force with local law enforcement agencies in terms of memoranda of agreement or other agreements in place (describe), protection responsibilities defined (describe), communication procedures developed (describe), and participation in drills and exercises.	
2. What is the approximate response time for local law enforcement personnel?	

INFORMATION, COMPUTER, NETWORK, and INTELLECTUAL PROPERTY SECURITY

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Information, Computer, Network, and Intellectual Property Security	
1. Have steps been taken to protect technical and business information that could be of use to potential adversaries (sometimes referred to as operational security or OPSEC)?	
2. Have the documentation/computer files that need to be protected for confidentiality been systematically identified and regularly backed-up?	
3. Is sensitive information in research and development and laboratory areas safe-guarded against inadvertent disclosure?	
4. Is sensitive information in maintenance areas safeguarded against inadvertent disclosure?	
5. Are computers as well as disks, tapes, and other media adequately secured physically from theft?	
6. Are procedures followed to reduce the likelihood that spoken information (in face-to-face conversations, phone calls, and radio communications) could be picked up by adversaries?	
7. If the content of radio communications cannot be restricted for operational reasons, have they been voice-encrypted?	
8. Are user authorizations granted on the basis of "need to know," "least access," and "separation of functions" rather than position or precedent (note: this has to be balanced against the process safety concepts of employee access to process safety information and employee participation)?	

INFORMATION, COMPUTER, NETWORK, and INTELLECTUAL PROPERTY SECURITY (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
9. Are appropriate procedures followed for protecting and destroying sensitive documents that could provide key information on critical process operation or vulnerabilities?	
10. Is the computer/server room secured?	
11. Is the computer/server room on the second floor (to protect it from flooding and to reduce the likelihood of theft), and away from outside walls?	
12. Is the computer/server room equipped with adequate communications capability?	
13. Is access to the computer/server room limited to only authorized personnel who need entry?	
14. Are appropriate hardware, software, and procedural techniques used for protecting computers and networks, such as:	
a. Firewalls?	
b. User ID?	
c. Password controls, including the regular changing of passwords?	
d. Encryption?	
15. Virus protection?	
16. Are computer transaction histories periodically analyzed to look for irregularities that might indicate security breaches?	
17. Is Internet access disabled in all application software or operating systems that are prepackaged?	

INFORMATION, COMPUTER, NETWORK, and INTELLECTUAL PROPERTY SECURITY (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
18. Are measures in place to control access to or otherwise secure process-specific operating information (e.g., including diagrams, procedures, control loop/DCS information), both electronic and hardcopy versions?	
19. Are process control systems protected from external manipulation (e.g., hacking into control system to operate equipment or delete or alter software codes)?	
20. Is access to process control systems via the Internet or Intranet been restricted? If access is allowed, is the access allowed only to the absolute minimum number of personnel necessary, using user ID, password, separate authentication, and encryption controls as appropriate?	
21. Are temporary passwords restricted from use except for new employees, or when a password is forgotten or is inactive?	
22. Are vendor-supplied passwords changed immediately after installation?	
23. Do users have screen saver with password available and in use when leaving computers on and unattended?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
(a) Hardening Processes	
1. Have existing security countermeasures been designed using the concept of rings of protection? Are the critical assets that may qualify as attractive targets at the center of concentric rings of layered protective features?	
2. Have process and systems been designed using the concept of layers of protection? Are there adequate independent protective layers that would detect, prevent, or mitigate a release of hazardous materials?	
3. Are critical process areas and equipment protected with traffic barriers, bollards, dikes, or other measures (e.g., diversionary structures that prevent vehicles from accelerating along a clear path to the process/equipment) to prevent ramming with vehicles?	
4. Are process "unit roads or streets" (i.e., roadways that provide access into specific process areas) provided with gates and, if so, are they securely closed when not in use (these gates may help limit direct vehicular access to critical equipment)?	
5. Are vehicles (except necessary material transport vehicles and/or authorized plant vehicles) prohibited from parking near critical process equipment (300 feet is considered a minimum distance)?	
6. Are full tank trailers or rail cars containing highly hazardous materials (i.e., those materials that could be targeted by terrorists) stored away from fence lines or perimeter areas to reduce their vulnerability to attack?	
7. Are full tank trailers or rail cars containing flammable or explosive materials stored away from critical process areas and equipment to prevent propagation of effects to critical processes?	
8. Are critical processes or equipment, such as tanks storing highly hazardous materials, protected from explosion or fire at adjacent processes (e.g., blast walls)?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
9. Is good housekeeping practiced in critical process areas and are trash dumpsters or receptacles located away from critical processes and equipment (trash dumpsters and poor housekeeping may make it easier to hide a bomb)?	
10. Are doors to interior buildings (e.g., process buildings) and control rooms locked or otherwise secured, where appropriate?	
11. Are hinge pins on doors to critical process areas on the inside of the door? (Note: May not be possible and still maintain easy egress in fire/emergency situations—doors must open out.)	
12. Are critical process areas surrounded with locked and secure fencing (in addition to site perimeter fencing) or located within locked buildings? (Note: Locked and secured fencing or buildings may create confined space issues.)	
13. If critical process areas are not surrounded by fencing or within buildings or if infeasible to do so, are the processes patrolled or monitored continuously by security personnel?	
14. Are highly reactive materials (e.g., water-reactive chemicals) stored in a location and manner that minimizes the potential for intentional contamination (e.g., stored in locked building away from water hose connections, situated away from pipelines/connections with potential incompatible chemicals)?	
15. Are key valves, pumps, metering stations, and open-ended lines on critical processes, especially those in remote or uncontrolled/ unrestricted areas, locked closed, located in locked secure structures (e.g., pump house), surrounded by locked secure fencing, and/or constructed of heavy-duty, tamper-resistant materials?	
16. Are ingredients for products potentially targeted for contamination unloaded, stored, transferred, and added to the process in a manner that is monitored and checked?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
17. Can exposed/remote equipment on critical processes feasibly be re-located to more secure/less vulnerable locations?	
18. Can critical process equipment that is highly recognizable from the ground and/or site perimeter be made less recognizable? (Note: This must be balanced against emergency responders need to readily identify equipment)	
19. Can critical processes or equipment be recognized readily from the air (consult aerial photos, if available) and, if so, can they be made less recognizable? (Note: This must be balanced against safety and code issues, such as painting of certain storage tanks in light colors.)	
(b) Reducing the Quantity and Hazard of a Release from a Malicious Act	
1. Has a review of site utility systems been conducted to identify and assess vulnerability of utilities that are essential to safe operation and shutdown of critical processes? Examples of possible critical utilities are:	
a. Electrical power	
b. Cooling water	
c. Compressed air	
d. Natural gas or other fuels	
e. Steam	
f. Nitrogen or other inert gases	
g. Secondary containment (drainage and sewer systems)	
h. Communications systems	
2. Are utility areas that can affect critical processes appropriately secured and monitored? (e.g., cooling water systems and agitation systems on reactive chemical processes that may be particularly important)	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
3. Where appropriate, has safe and rapid manual shutdown capability been provided for critical processes and utilities?	
4. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, is the operating status of the utilities monitored and/or to alert personnel (e.g., an alarm sounds when cooling water flow is lost or reduced below critical levels)?	
5. Where loss or reduction of utilities can potentially lead to uncontrolled reactions on critical processes, are feed systems interlocked to agitation, cooling systems, and other appropriate utilities in the event of loss of those utilities or systems?	
6. Are appropriate back-up power supplies available for critical processes to allow a safe shutdown? (Note: UPS can be compromised by adversaries.)	
7. In the event of loss of power or pneumatics, do valves and other equipment fail to a safe position in critical processes?	
8. Are container storage areas secured or otherwise monitored, especially those outside of process buildings or in remote areas? (Note: A fire or explosion involving multiple containers can lead to smoke/combustion by-products that present off-site hazards and can serve as a diversion or a "statement.")	
9. Have storage and process inventories of hazardous chemicals been reduced to the extent practicable?	
10. Where appropriate, are critical processes containing highly hazardous chemicals "segmented" (either automatically or via manual action) to prevent release of the majority of process contents (i.e., only the quantity in the compromised "segment" would be released)?	
11. Are pipelines containing highly hazardous materials equipped with low-pressure interlock systems that shut valves or take other action to minimize the release quantity?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
12. Are open-ended lines or other lines or vessel drain systems on critical processes equipped with excess flow valves?	
13. Where appropriate, are hazardous materials being procured in smaller containers instead of maintaining large inventories in a single vessel?	
14. Has a review been conducted to determine if hazardous materials can be purchased and used in a less hazardous form? (Note: This may be particularly applicable to solvents/carriers and waste or water treatment chemicals.)	
15. If materials can be purchased and used in less hazardous forms, is this approach being addressed in an expedited manner?	
16. Has the feasibility and merit of storing large inventories of highly hazardous materials in underground tanks or other systems (e.g., aboveground vaults) that would limit the release rate been evaluated? (Note: This must be balanced against environmental concerns and other liabilities.) If found to be of merit, are plans in place to pursue this approach?	
17. Where appropriate and feasible, are tanks, vessels, and tank trailers/rail cars disconnected from delivery or transfer piping when not in use? (Note: The piping may be more vulnerable than the vessel.)	
(c) Mitigating a Release from a Malicious Act	
1. Are appropriate passive mitigation systems in-place for addressing large volume releases from critical processes?	
2. Have passive mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
3. Has passive leak-limiting technology been used where possible (e.g., gaskets resistant to blowout, excess flow valves, etc.)?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
4. Are appropriate active mitigation systems in-place for addressing large volume releases at critical processes?	
5. Have active mitigation systems been assessed for integrity (i.e., are they being tested and/or maintained as required periodically) and vulnerability to be compromised?	
6. Are key control valves, pumps, and other equipment associated with active mitigation systems been locked or secured in operational/ready positions or located within secure structures?	
7. Has expanding the areas of the site where potential ignition sources are limited or eliminated (e.g., expanding the area of site subject to Class I/Div 1 or 2 electrical classification) been evaluated?	
(d) Emergency Response, Crisis Management, and Community Coordination	
1. Is the site's emergency response plan updated for current personnel and organizational functions?	
2. Do emergency plans address security worst case events, or events that are equivalent to security worst case events?	
3. Do emergency plans address malicious acts, especially responder actions in the event of a suspected terrorist/saboteur attack?	
4. Do emergency shutdown procedures address actions to take in the event of catastrophic releases or other terrorist-type event to safely shutdown the process and limit the release? If not, are shutdown procedures being reviewed and updated accordingly?	
5. Does the crisis management plan account for events such as:	
a. Bomb threats?	
b. Elevated homeland security warning status?	
c. Civil disturbance?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continued)

Date: [MONTH XX, 2002] Facility: [FACILITY]	
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
6. Are operating personnel trained in the above-referenced emergency shutdown procedures, especially where they have been updated to address catastrophic or terrorist events?	
7. Has emergency equipment stationed near critical processes (e.g., hose connections) been assessed for vulnerability to compromise and, where appropriate, secured, monitored, or otherwise protected?	
8. If responding to a malicious act, are emergency responders aware that secondary "sucker-punch" devices (i.e., additional incendiary/explosive devices) or effects may be present if flammables are released or explosions are involved?	
9. Are procedures in-place (and responders trained accordingly) to address preservation of evidence due to the area being considered a crime scene?	
10. Where other nearby targets may exist (especially those that may present a greater risk than processes at our site), are plans in place to coordinate with local responders to ensure that those targets are monitored or otherwise protected in the event of a potential "diversionary" attack on our site?	
11. Have plans been developed with adjacent or nearby industry and local officials to facilitate timely communication of suspicious activity between potentially concerned parties?	
12. Have evacuation and shelter-in-place plans been fully developed and coordinated with local offsite emergency responders?	
13. Have local residents and business been instructed on how to shelter-in-place?	
14. Are local police, fire departments, health care providers, and other emergency responders aware of the hazardous materials at the site?	

PREVENTING AND CONTROLLING RELEASES OF HAZARDOUS MATERIALS (Continue

Date: [MONTH XX, 2002]	Facility: [FACILITY]
This checklist applies to [the entire facility/ASSET]	
	COMMENTS
15. Are plans in place to communicate information to local offsite emergency responders and officials in the event of a release?	
16. Do periodic emergency drills address malicious acts or other security-related emergencies?	
17. Is there a drill/exercise critique system in place to assure that experience from drills and actual emergencies are incorporated into the emergency response plan?	